An Introduction to
NECCC E-SIGN Interoperability Workgroup and
State Electronic Records and Signatures Reciprocity and Interoperability Issues

Background

> The legality of an electronically signed record requires that it "**remains accessible to all persons who are entitled to access** by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise." *(emphasis added)*
>
> *•Federal Electronic Signatures in Global and National Commerce Act, Section101. (d)(1)(B) (E-SIGN - interstate and international commerce)*

> "Visionary leadership, joined with thoughtful planning and monitoring, can make e-government a useful vehicle for government services and information. Ideally, government leaders will establish a central authority (Chief Information Officer [CIO] and/or a governance council) with responsibility for setting a unified direction for developing e-government."
>
> *Critical Business Issues In the Transformation to Electronic Government*[1], Issue #1 Leadership/Governance, NECCC 2000 report, page 5

Using electronic signatures means creating signed electronic documents. This work group asked "how do we get from technology neutral e-signatures statutes to agreement about what are sharable, trustworthy signed electronic documents (things that are reliable, usable, authentic, and having integrity)?"

The Interoperability work group defined the essential requirements for a formally formed electronic record and signature as follows:

Secure electronic signatures

A signature is a secure electronic signature if, through the application of a security procedure, it can be demonstrated that the electronic signature at the time the signature was made was all of the following:

1. Unique to the person using it.
2. Capable of verification.
3. Under the sole control of the person using it.
4. Linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.

Secure electronic records

If, through the ongoing application of a security procedure, it can be demonstrated that an electronic record signed by a secure electronic signature has remained unaltered since a specified time, the record is a secure electronic record from that time of signing forward.

The work group recognized that there are many processes to form these signatures and documents. There are also varying levels of certainty desired for identifying a person, attributing a signature to them and assuring the integrity of the signed document. The Interoperability work group explicitly expects that once the general agreement on forms

---

[1] *NECCC Audit Guidance Committee*: Chair Nancy Rainosek, TX, State Auditor's Office and Co-chair Joe Moore, AZ, Office of the Auditor General

of electronic signature and records are reached, other business purpose specific interoperability groups (existing or formed) will work to find common sharing methods consistent with the general requirements. These specific interoperability groups would focus on specific issues (e.g. electronic notary, EPA reporting, IRS/state revenue reporting systems, electronic vehicle title transfer).

Scope of work group effort

The work group developed a framework for moving from technology neutral e-signatures statutes to agreement between states about what are sharable, trustworthy signed electronic documents. But before a state can look outward, it will need to determine the general policy and governance framework for electronic signature use within the state's agencies and those conducting business with those agencies.

A critical question is, to advance electronic government initiatives, how do we, as responsible parties in state government, address the need to know who is doing business with state systems so we can manage confidential information and ensure the integrity of transactions. We must protect the information we store, while making certain that authorized individuals are held accountable for what is reported. Someone must "sign the dotted line" to initiate and accept transactions. We must be able to guarantee that a signed document has legal effect, both for sender and receiver, within our states and beyond our state borders.

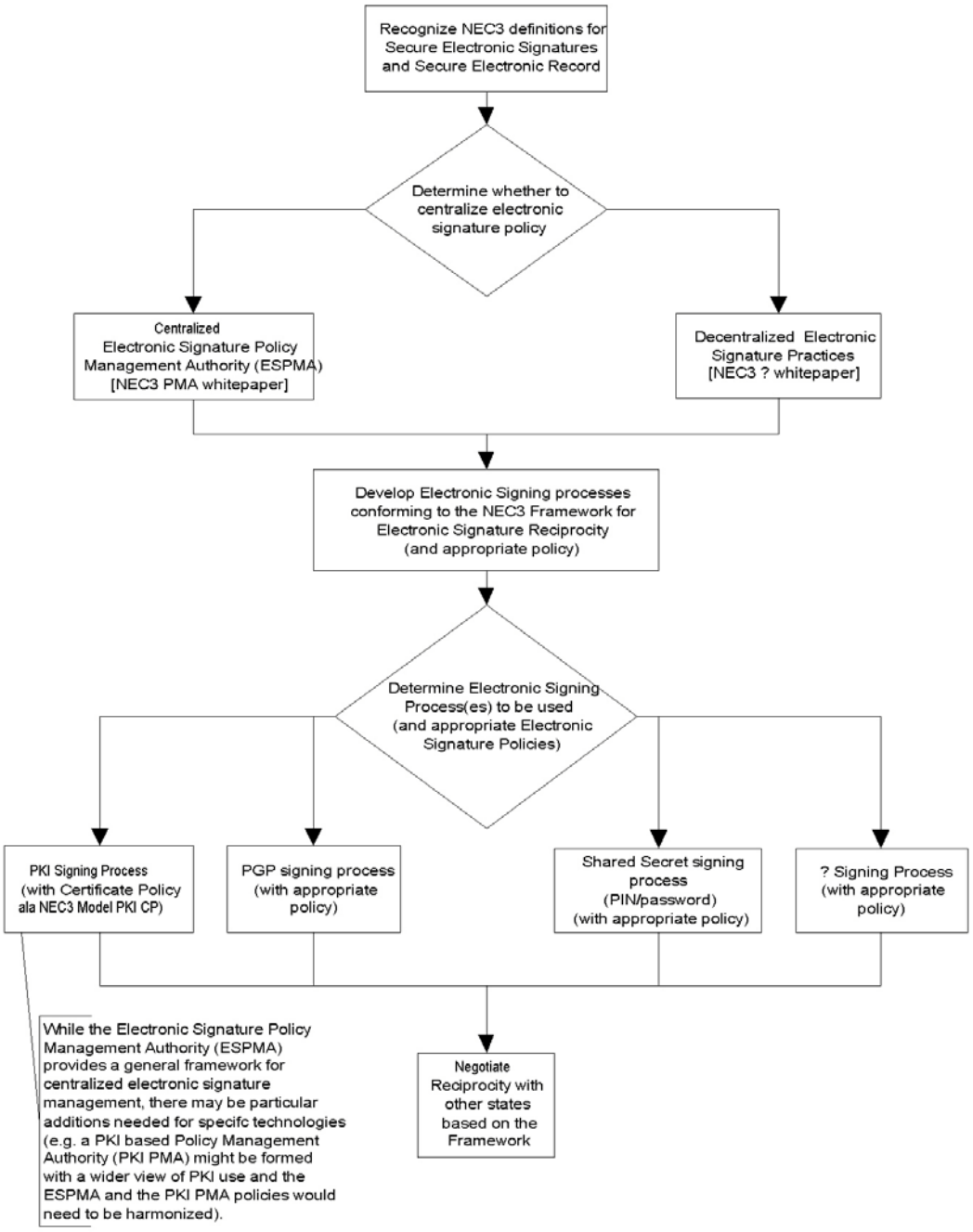
Creating a workable and secure system for electronic government requires an Electronic Signature Infrastructure (ESI) to integrate policy, procedures, people and technology. This human and technical resource integration within an ESI serves to authenticate the signing parties, encrypt transactions to ensure confidentiality, and communicate the processes for signing with legal intent. Due to the varied ways in which states assign responsibilities to multiple and overlapping authorities, it is certain that States will take different approaches to the distribution of authority for these functions. As we have seen so far, the states who have demonstrable need for reciprocity are driven by the applications and relationships among stakeholders in the projects they choose to implement. Some states, however, are hesitant to embark on projects without having an infrastructure in place that will ensure compatibility for future applications, applications whose technology cannot be known at this time.

The integration required for interoperability and legal transference of signed documents within and among states over time, over multiple applications, requires central coordination of policies, a repository of stakeholder agreements, processes, and contracts. And, in the opinion of the Interoperability Working Group, this integration also requires a single point of view, as articulated by each state's Electronic Signature Policy Management Authority (for purposes of this document, the ESPMA, or, The Authority).

In order for a state to determine whether to choose the centralized or decentralized model, we have included a graphic depicting the decision points for helping a state determine the appropriate direction. We have also developed papers for selected points on the path toward electronic signature reciprocity between states.

DRAFT v0.5

Proposed Process leading to Electronic Signature Reciprocity between States



The intent of using the term “model” (e.g. "Model PKI CP") is to suggest having a framework *inside* a state that can then readily connect to a similar framework inside *another* state. The similarity in framework can be more readily judged by having a generally agreed on “model” to compare each to.

Our hope is that all parties will recognize the need to integrate policy, procedures, people and technology *and* the need to do so in similar ways while remaining flexible enough to adapt to new signing processes as the underlying technologies evolve. That is the goal of this series of papers.